# CLAIMS

1. A method for implementing port-based network access control at a shared media port in an intermediate node, the shared media port being coupled to a plurality of client nodes, the method comprising:

partitioning the shared media port into a plurality of logical subinterfaces, each logical subinterface dedicated to providing access to a different network or subnetwork accessible through the intermediate node;

receiving a data packet at the shared media port from a first client node;

associating the received data packet with a first logical subinterface in the plurality of logical subinterfaces;

determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork; and

if the first client node is determined to be authenticated to communicate over the first logical subinterface's dedicated network or subnetwork, forwarding the received data packet over the first logical subinterface's dedicated network or subnetwork.

2. The method according to claim 1, further comprising:

performing at least one of dropping the received data packet or reclassifying the received data packet to a different logical subinterface, if the first client node is determined not to be authenticated to communicate over the first logical subinterface's dedicated network or subnetwork.

3. The method according to claim 1, wherein the first logical subinterface's dedicated network or subnetwork is a virtual private network (VPN).

4. The method according to claim 1, wherein a logical subinterface in the plurality of logical subinterfaces is dedicated to providing access to the Internet.

5. The method according to claim 1, wherein the step of determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork further comprises:

parsing a source media access control (MAC) address from the received data packet;

indexing an entry in a MAC filter associated with the shared media port based on the value of the parsed source MAC address;

identifying an authentication state stored in the indexed MAC-filter entry; and

determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork based on the authentication state stored in the indexed MAC-filter entry.

6. The method according to claim 5, wherein the MAC filter is organized as a hash table.

7. The method according to claim 1, further comprising:

parsing a destination Internet Protocol (IP) address from the received data packet;

comparing the parsed destination IP address to one or more IP addresses stored in an IP filter associated with the shared media port; and

if the parsed destination IP address matches an IP address stored in the IP filter, forwarding the received data packet over the first logical subinterface's dedicated network or subnetwork, even if the first client node is determined not to be authenticated to communicate over that network or subnetwork.

8. The method according to claim 1, wherein the step of associating the received data packet with the first logical subinterface, further comprises:

locating an entry in a routing table configured to store routing information associated with the received data packet; and

associating the received data packet with the first logical subinterface based on the contents of the routing-table entry.

9. The method according to claim 1, further comprising:

receiving an authentication request from the first client node at the shared media port;

in response to receiving the authentication request, creating a MAC filter associated with the shared media port if the MAC filter has not already been created;

copying a source MAC address stored in the received authentication request into an appropriate entry in the MAC filter;

forwarding the received authentication request to an authentication service;

receiving a response from the authentication service, the response identifying an authentication state associated with the first client node; and

storing the authentication state into the same MAC-filter entry into which the source MAC address was copied.

10. The method according to claim 9, wherein the step of copying the source MAC address into an appropriate MAC-filter entry further comprises:

indexing an entry in the MAC filter based on the result of applying a hash function to the source MAC address; and

storing the source MAC address at the indexed MAC-filter entry.

11. The method according to claim 9, wherein the received authentication request is an 802.1X authentication request.

12. The method according to claim 9, further comprising:

sending an alarm message over the first logical subinterface's dedicated network or subnetwork after the first client node fails to authenticate at the shared media port a predetermined number of times.

13. The method according to claim 9, further comprising:

sending an alarm message over the first logical subinterface's dedicated network or subnetwork after the first client node's authentication state changes from an authenticated state to an unauthenticated or unknown state.

14. An intermediate node for implementing port-based network access control in a network containing a plurality of client nodes, the intermediate node comprising:

a processor;

a shared media port for receiving a data packet from a first client node in the plurality of client nodes; and

a memory adapted to store instructions for execution by the processor, at least a portion of the instructions defining a network operating system configured to perform the steps of:

partitioning the shared media port into a plurality of logical subinterfaces, each logical subinterface dedicated to providing access to a different network or subnetwork accessible through the intermediate node;

associating the data packet received from the first client node with a first logical subinterface in the plurality of logical subinterfaces;

determining whether the first client node is authenticated to communicate over the network or subnetwork to which the first logical subinterface provides dedicated access; and

forwarding the received data packet over the first logical subinterface's dedicated network or subnetwork only if the first client node is determined to be authenticated to communicate over that network or subnetwork.

15. The intermediate node according to claim 14, wherein:

the memory is further adapted to store a MAC filter containing one or more entries configured to store at least a MAC address and an authentication state, and

the network operating system is further configured to perform the steps:

receiving an authentication request from the first client node at the shared media port;

copying a source MAC address stored in the received authentication request into an appropriate entry in the MAC filter;

forwarding the received authentication request to an authentication service;

receiving a response from the authentication service, the response identifying an authentication state associated with the first client node; and

storing the authentication state into the same MAC-filter entry into which the source MAC address was copied.

16. The intermediate node according to claim 14, wherein:

the memory is further adapted to store an IP filter containing a list of IP addresses, and

the network operating system is further configured to perform the steps:

parsing a destination IP address from the received data packet;

comparing the parsed destination IP address to one or more IP addresses stored in an IP filter associated with the shared media port; and

if the parsed destination IP address matches an IP address stored in the IP filter, forwarding the received data packet over the first logical subinterface's dedicated network or subnetwork, even if the first client node is determined not to be authenticated to communicate over that network or subnetwork.

17. The intermediate node according to claim 14, wherein:

the memory is further adapted to store a MAC filter containing one or more entries configured to store at least a MAC address and an authentication state, and

the network operating system is further configured to perform the steps:

parsing a source MAC address from the received data packet;

indexing an entry in a MAC filter associated with the shared media port based on the value of the parsed source MAC address;

identifying an authentication state stored in the indexed MAC-filter entry; and

determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork based on the authentication state stored in the indexed MAC-filter entry.

18. An apparatus that implements port-based network access control at a shared media port, the shared media port being coupled to a plurality of client nodes, the apparatus comprising:

means for partitioning the shared media port into a plurality of logical subinterfaces, each logical subinterface dedicated to providing access to a different network or subnetwork accessible through the intermediate node;

means for receiving a data packet at the shared media port from a first client node;

means for associating the received data packet with a first logical subinterface in the plurality of logical subinterfaces;

means for determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork; and

means for forwarding the received data packet over the first logical subinterface's dedicated network or subnetwork.

19. The apparatus according to claim 18, wherein the means for determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork further comprises:

means for parsing a source MAC address from the received data packet;

means for indexing an entry in a MAC filter associated with the shared media port based on the value of the parsed source MAC address;

means for identifying an authentication state stored in the indexed MAC-filter entry; and

means for determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork based on the authentication state stored in the indexed MAC-filter entry.

20. The apparatus according to claim 18, further comprising:

means for parsing a destination IP address from the received data packet;

means for comparing the parsed destination IP address to one or more IP addresses stored in an IP filter associated with the shared media port; and

means for forwarding the received data packet over the first logical subinterface's dedicated network or subnetwork, even if the first client node is determined not to be authenticated to communicate over that network or subnetwork.

21. The apparatus according to claim 18, wherein the means for associating the received data packet with the first logical subinterface, further comprises:

means for locating an entry in a routing table configured to store routing information associated with the received data packet; and

means for associating the received data packet with the first logical subinterface based on the contents of the routing-table entry.

22. The apparatus according to claim 18, further comprising:

means for receiving an authentication request from the first client node at the shared media port;

means for creating a MAC filter associated with the shared media port if the MAC filter has not already been created;

means for copying a source MAC address stored in the received authentication request into an appropriate entry in the MAC filter;

means for forwarding the received authentication request to an authentication service;

means for receiving a response from the authentication service, the response identifying an authentication state associated with the first client node; and

means for storing the authentication state into the same MAC-filter entry into which the source MAC address was copied.

23. The apparatus according to claim 22, wherein the received authentication request is an 802.1X authentication request.

24. A computer-readable media including instructions for execution by a processor, the instructions for a method of implementing port-based network access control at a

shared media port in an intermediate node, the shared media port being coupled to a plurality of client nodes, the method comprising the steps:

partitioning the shared media port into a plurality of logical subinterfaces, each logical subinterface dedicated to providing access to a different network or subnetwork accessible through the intermediate node;

receiving a data packet at the shared media port from a first client node;

associating the received data packet with a first logical subinterface in the plurality of logical subinterfaces;

determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork; and

if the first client node is determined to be authenticated to communicate over the first logical subinterface's dedicated network or subnetwork, forwarding the received data packet over the first logical subinterface's dedicated network or subnetwork.